JPL:JBD
F. #2023R00495

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR AUTHORIZATION TO SEARCH (1) A BLACK APPLE IPHONE WITH IMEI NUMBER 350320348076355; (2) A BLACK ANDROID CELLPHONE WITH IMEI NUMBER 354090791398384; (3) A GRAY APPLE MACBOOK LAPTOP; (4) A BLUE SAMSUNG PORTABLE HARD DRIVE, T7 SSD; (5) A BLACK SAMSUNG PORTABLE HARD DRIVE, T7 SSD; (6) A 128 GB SANDISK SD MEDIA CARD; (7) A 128 GB PROGRADE SD MEDIA CARD, ALL IN LAW ENFORCEMENT CUSTODY WITHIN THE EASTERN DISTRICT OF NEW YORK	**APPLICATION FOR A SEARCH WARRANT** Case No. 23-MJ-644

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Thomas Jacques, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—six electronic devices, described below and in Attachment A—that is currently in law enforcement custody in the Eastern District of New York, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Department of Homeland Security, Homeland Security Investigations ("HSI"), and have been since December 2016. I am assigned to the Child Exploitation Investigations Unit. During my tenure with HSI, I have participated in the investigation of cases involving crimes against children. Specifically, I have experience investigating cases involving production, receipt, distribution, and possession of child pornography and have conducted physical and electronic surveillance, executed search warrants, reviewed and analyzed electronic devices, and interviewed witnesses. As part of my employment with HSI, I successfully completed the Federal Law Enforcement Training Center's Criminal Investigator Training Program and Immigration and Customs Enforcement Special Agent Training, both of which included instruction with respect to the application for, and execution of, search and arrest warrants, as well as the application for criminal complaints, and other legal processes. As a result of my training and experience, I am familiar with the techniques and methods of operation used by individuals involved in criminal activity to conceal their actions from detection by law enforcement.

3. This affidavit is based upon my personal knowledge, my review of documents and other evidence, and my conversations with other law enforcement officers, as well as my training and experience. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

4. This affidavit is intended to show only that there is probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

5. The property to be searched is (1) a black Apple iPhone with International Mobile Equipment Identity ("IMEI") number 350320348076355 (the "Black iPhone"); (2) a black Android cellphone with IMEI number 354090791398384; (3) a gray Apple Macbook laptop; (4) a blue Samsung portable hard drive, T7 SSD; (5) a black Samsung portable hard drive, T7 SSD; (6) a 128 gigabyte Sandisk SD media card; (7) a 128 gigabyte Prograde SD media card (collectively, the "SUBJECT DEVICES"). The Black iPhone was seized incident to the arrest of the defendant Douglas Noel ("NOEL") on July 10, 2023. The remaining SUBJECT DEVICES were seized from NOEL on or about June 28, 2023 by police in Clarkstown, New York when NOEL was detained and questioned after he attempted to meet a person he believed to be a 13-year-old girl at a hotel in Nanuet, New York. The remaining SUBJECT DEVICES were transferred to HSI custody on July 11, 2023. From my training and experience, I know that the SUBJECT DEVICES have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the SUBJECT DEVICES first came into law enforcement's possession.

PROBABLE CAUSE

6. Based upon the information below, there is probable cause to believe that violations of Title 18, United States Code, Sections 2422(b) (coercion and enticement of a

minor), 2251 (sexual exploitation of children) and 2252A(a)(2)(A) (receipt of child pornography) (the "SUBJECT OFFENSES") have been committed by Douglas Noel ("NOEL") and that the SUBJECT DEVICES contain evidence of the SUBJECT OFFENSES.

7. On or about May 1, 2023, HSI created an Instagram account that was intended to appear as though it belonged to a 15-year-old girl (the "Undercover Account"). The Undercover Account indicated that the user was a 15-year-old girl in Springfield, Massachusetts; featured several pictures of an undercover female agent that were filtered to make the agent appear younger; and included the hashtags, "#15thbirthday, #teenmodel, #teenfashion and #girl."

8. On or about May 4, 2023, an Instagram account with the username "dougnoel.photography" (the "NOEL Account") posted a comment on one of the photographs on the Undercover Account, saying, "You're very pretty. I'd love to do a photoshoot with you." As explained further below, I understand NOEL to be the user of the NOEL Account. Over the next several days, NOEL and the Undercover Account proceeded to exchange several direct messages over Instagram. HSI agents sent all messages from the Undercover Account. Among other things, on or about May 6, 2023, NOEL asked the Undercover Account, in sum and substance, to come stay with him at his apartment in New York City for the weekend. Later that day, the Undercover Account told NOEL that she was only 15 years old, to which NOEL responded, "I

kind of figured with the whole mom thing[1] . . . I don't mind you being 15. I still think you're gorgeous." Later on, NOEL wrote, "TBH, I saw the tag about your 15th birthday in your first post, so I figured you'd just turned 15. But by then we'd already been talking about visiting and I didn't want to come across as a crop [sic] by mentioning it. Cause I really like you."

9. A few days later, on or about May 8, 2023, NOEL began making explicitly sexual comments to the Undercover Account. Among other things, NOEL wrote, "well I guess I can admit now that I've had a crush on you for a while now. And I really want to kiss you . . . Do you want me to teach you about sex and take your virginity?" Later that same day, NOEL wrote, "We would go slow. Explore each other's bodies. I'd suck on your nipple and kiss you. Touch you. Make you feel good before we even have sex."

10. Shortly thereafter, beginning on or about May 12, 2023, NOEL began asking the Undercover Account to send him sexually explicit pictures. Initially, NOEL asked the Undercover Account to send him pictures of her breasts, which the Undercover Account did not do. NOEL and the Undercover Account remained in contact for the next several weeks, and on or about June 5, 2023, NOEL wrote to the Undercover Account, among other things, "You could go to the bathroom or your bedroom and take your shirt and bra off and pinch your nipples and take a selfie for me. And if you want to spread your 15-year-old pussy open for me that would

---

[1] I understand NOEL's reference to "the mom thing," to refer to an earlier statement by the Undercover Account that her mother was going away in June and that she would be home alone at that time.

turn me on so much. If you wanted to rub your clit for me and say 'fuck my 15 year old pussy with your 45 year old cock daddy' in a little video that would very hot too." The Undercover Account then indicated to NOEL that the Undercover Account had taken pictures requested by NOEL but did not want to send them. NOEL subsequently wrote to the Undercover Account, "I've been thinking about those pictures you took. It's so hot you did that for me. I was thinking you could send them so they would disappear." No photographs were ever taken or sent by the Undercover Account.

11. On or about June 8, 2023, an undercover officer conducted a live video call with NOEL. The call was recorded. That call provided a clear view of NOEL's face, which HSI agents compared to pictures of NOEL from the Department of Motor Vehicles and confirmed that the person was, in fact, NOEL. Additionally, NOEL was wearing brown glasses and a dark red t-shirt. Among other things, during that call, NOEL asked the undercover officer if she was "nervous about us having sex for the first time" and proceeded to discuss taking naked pictures of the undercover officer when they met up. When NOEL asked the undercover officer what grade she was in, the undercover officer responded that she did not want to tell him. NOEL then responded, "you're afraid that I won't want to have sex with a middle school girl but I do."

12. Pursuant to a judicially authorized search warrant issued by the Honorable Katherine Robertson, United States Magistrate Judge for the District of Massachusetts, Meta provided HSI with information regarding the NOEL Account indicating that NOEL has attempted to entice or solicit other individuals identifying as minor children. For example, in

messages with an Instagram user who identified herself to NOEL as a 13-year-old female, NOEL wrote, among other things, "I'd have slid my adult cock into your child pussy at 11 for sure . . . say rape my 13 year old underage pussy with your 44 year old cock . . . I know it's wrong to have sex with 13 year old girls but I'm going to fill all three of you with my cum . . . I want to make child porn with you." In another chat with an individual who identified herself to NOEL as a 15-year-old female, NOEL wrote, among other things, "Would you want me to touch you when you were 8? . . . May I see you naked beautiful? . . . Would you spread your legs for me so I can use your child pussy."

13. Additionally, Meta indicated that the chats referenced above came from the internet protocol ("IP") address 67.250.86.135. In response to a subpoena, Charter Communications, Inc. indicated that the 67.250.86.135 IP address was subscribed to by NOEL at a home he rented in the Astoria neighborhood of Queens, New York (the "Astoria Residence"). HSI agents subsequently obtained a judicially authorized warrant for prospective location data for NOEL's cellular telephone. Data obtained as a result of that warrant indicates that NOEL was regularly inside the Astoria Premises, and that he was in the Astoria Premises during the June 8, 2023 video call with the undercover agent posing as a minor female.

14. On June 28, 2023, the Honorable Vera M. Scanlon, United States Magistrate Judge for the Eastern District of New York, signed an application authorizing the search of the Astoria Premises, including for any electronic devices found therein (the "June 28 Warrant").

15. Also on or about June 28, 2023, NOEL traveled to a hotel in Nanuet, New York to meet a person he had been exchanging sexually explicit messages with on the Telegram Messenger application who had identified herself to him as a 13-year-old girl. When NOEL arrived at the hotel, he was met by members of the group "Predator Poachers," a non-governmental group comprised of private citizens that attempts to uncover sexual abusers of children over the internet. Members of Predator Poachers had been posing as the 13-year-old girl during conversations with NOEL over Telegram. Members of Predator Poachers called the Clarkstown police.[2] When the Clarkstown police arrived at the hotel, they found that NOEL was carrying (1) condoms, (2) emergency contraception, (3) erectile dysfunction medication, (4) a vibrator; (5) a bathing suit for a teenage girl, (6) a digital camera that accepts SD cards, and (7) the SUBJECT DEVICES, except for the Black iPhone—all of which they seized from NOEL. NOEL admitted to members of the Predator Poachers and to law enforcement that he had traveled to Nanuet to meet with someone he believed was 13 years old and that he had been engaging in sexually explicit conversations with individuals he believed to be minors over the internet. The Clarkstown police subsequently released NOEL to Nyack Hospital after NOEL expressed suicidal thoughts to officers.

---

[2] Prior to notifying the Clarkstown police, the Predator Poachers acted without prior knowledge or authorization of law enforcement and therefore did not act subject to law enforcement's control or direction, or on behalf of law enforcement.

16. HSI learned about NOEL's attempt to meet with a 13-year-old girl at the hotel in Nanuet on July 3, 2023. On or about July 5, 2023, agents from HSI attempted to execute the June 28 Warrant on the Astoria Residence. When agents arrived, they found the Astoria Residence was empty and learned from NOEL's landlord that NOEL had moved to an apartment in the Bushwick neighborhood of Brooklyn, New York (the "Bushwick Residence").

17. On July 10, 2023, upon application of the government, the Honorable Sanket J. Bulsara, United States Magistrate Judge for the Eastern District of New York, issued a warrant for NOEL's arrest pursuant to a criminal complaint charging one count of attempted sexual exploitation of a minor, in violation of Title 18, United States Code, Sections 2251(a) and 2251(e). HSI arrested NOEL pursuant to that warrant the following day. The Black iPhone was seized from NOEL incident to his arrest.

18. Based on the information described above, I respectfully submit that probable cause exists to believe that NOEL committed the SUBJECT OFFENSES by, among other things, sending sexually explicit messages to Instagram users who have identified themselves to him as minor children; asking those Instagram users to send him child sex abuse material; indicating to those Instagram users that he would like to meet them in person to engage in sexual conduct; using Telegram to send sexually explicit messages to at least one person that he believes to be a minor child; and traveling to meet with a person he believed to be a minor child and intending to sexually abuse that child.

19. Moreover, I respectfully submit that probable cause exists to believe that evidence of the SUBJECT OFFENSES will be found in the SUBJECT DEVICES. The information above indicates that NOEL routinely used one or more electronic devices to contact minor children and solicit sex and sexually explicit material from an IP address connected to his residence. Likewise, NOEL's reference to conducting a "photoshoot" with the undercover agent who he thought was a 15-year-old girl—and his bringing a camera to meet with a person he believed was a 13-year-old girl—indicates that the SUBJECT DEVICES likely contain images and other evidence relating to, among other things, child sex abuse material. The cell phones seized from the defendant include cameras, which can be used to produce child pornography, and the hard drives and flash drives can be used to store such material. I therefore respectfully submit that there is probable cause to search and seize evidence from the SUBJECT DEVICES.

TECHNICAL TERMS

20. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless

telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can

also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records of the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for

entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include GPS technology for determining the location of the device.

f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

21. Based on my training, experience and research, I know that some of the SUBJECT DEVICES have capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, GPS navigation device and PDA. In my training and experience,

examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the SUBJECT DEVICES.

COMPUTERS, ELECTRONIC STORAGE AND FORENSIC ANALYSIS

22. As described above and in Attachment B, this application seeks permission to search for records on a computer hard drive.

23. Based on my knowledge, training, and experience, I know that computers and electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

24. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the SUBJECT DEVICES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

25. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the SUBJECT DEVICES consistent with the warrant. The examination may require authorities to employ

techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the SUBJECT DEVICE to human inspection in order to determine whether it is evidence described by the warrant.

26. *Manner of execution.* This warrant seeks permission to search the SUBJECT DEVICES, which are already in law enforcement custody. I therefore submit that there is reasonable to conduct the seizure at any time, day or night.

CONCLUSION

27. I submit that the evidence described in this affidavit—which among other things shows NOEL repeatedly requesting child sexual abuse material on Instagram and other

electronic messaging applications, from individuals who identify themselves to him as minor children and detailing his intent to engage in sexual conduct with those minor children—supports probable cause for a warrant to search the SUBJECT DEVICES described in Attachment A and to seize the items described in Attachment B.

Respectfully submitted,

/s/ Thomas Jacques

Thomas Jacques
Special Agent
Homeland Security Investigations

Subscribed and sworn to me telephonically on
July 14, 2023:

Hon. Ramon E. Reyes, Jr. Digitally signed by Hon. Ramon E. Reyes, Jr.
Date: 2023.07.14 17:51:23 -04'00'

HONORABLE RAMON E. REYES, JR.
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

The property to be searched is (1) a black Apple iPhone with International Mobile Equipment Identity ("IMEI") number 350320348076355 (the "Black iPhone"); (2) a black Android cellphone with IMEI number 354090791398384; (3) a gray Apple Macbook laptop; (4) a blue Samsung portable hard drive, T7 SSD; (5) a black Samsung portable hard drive, T7 SSD; (6) a 128 gigabyte Sandisk SD media card; (7) a 128 gigabyte Prograde SD media card (collectively, the "SUBJECT DEVICES").

ATTACHMENT B

1. All information or records relating to violations of Title 18, United States Code, Sections 2422(b) (coercion and enticement of a minor), 2251 (sexual exploitation of children) and 2252A(a)(2)(A) (receipt of child pornography) (the "SUBJECT OFFENSES") involving Douglas Noel ("NOEL") and for the limited period from January 1, 2023 through the present, including the following:

a. Evidence concerning the commission of the SUBJECT OFFENSES, including but not limited to communications with individuals who appear or identify themselves to NOEL as minor children that are sexual in nature, and child pornography.

b. Records and information relating to access of Instagram, Telegram, Snapchat, Discord and other similar mobile applications.

c. Contact information, including names, phone numbers, and addresses, for victims or other individuals or places related to the SUBJECT OFFENSES;

d. Evidence of incoming and outgoing calls related to the SUBJECT OFFENSES;

e. Opened and unopened voicemail messages related to the SUBJECT OFFENSES;

f. Photographs or videos related to the SUBJECT OFFENSES, including but not limited to child pornography;

g. Emails, text, data, chat, digital photographs and video, MMS, SMS, or messages on social media or messaging applications installed on the device (collectively, "text messages"), any attachments to those text messages, such as digital photographs and videos, and any associated information, such as the phone number or user ID from which the text message was sent, pertaining to the SUBJECT OFFENSES;

h. Notes, documents, records, invoices, bank statements, or correspondence in any format, such as chat logs, electronic messages, and web cache information, related to the SUBJECT OFFENSES;

i. Calendar or other scheduling information related to the SUBJECT OFFENSES (including but not limited to itineraries and meetings with victims or other individuals and places related to the SUBJECT OFFENSES);

j. Browsing and search history, including cookies, related to the SUBJECT OFFENSES;

k. Cell tower, GPS and other location data relating to the SUBJECT OFFENSES.

l. Evidence of user attribution showing who used or owned the SUBJECT DEVICES at the time the things described in the warrant were created, edited or deleted, such as logs, phonebooks, saved usernames and passwords, documents and browsing history.

For computers and storage media whose seizure is authorized by this warrant, and any computer or storage media that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in

addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigative agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.